DATA SHEET

AI Threat Insights

Comprehensive, advanced threat detection & user entity behavior analysis

Modern organizations face daunting challenges protecting proprietary data and information against an increasingly sophisticated cybersecurity landscape. Businesses that rely on easily outdated static rules and malware signatures are vulnerable to zero-day attacks, insider threats, and other malicious activities. Today, IT pros need quick, actionable information based on proactive and automatic searches for security issues – before those issues become problems.

AI Threat Insights proactively monitors, detects, and prioritizes suspicious activity such as data exfiltration, port scans, application usage anomalies, and zero-day behaviors, and alerts admins to suspicious activity, threats, and vulnerabilities.

It is fully integrated with Absolute's broader Secure Access SSE platform, which includes Zero Trust Network Access with dynamic policy enforcement, remote browser isolation, content disarm and reconstruction, AV scanning, distributed firewalls, multi-factor authentication, optimized secure tunneling for enhanced security, and over 60 dashboards for deep visibility.

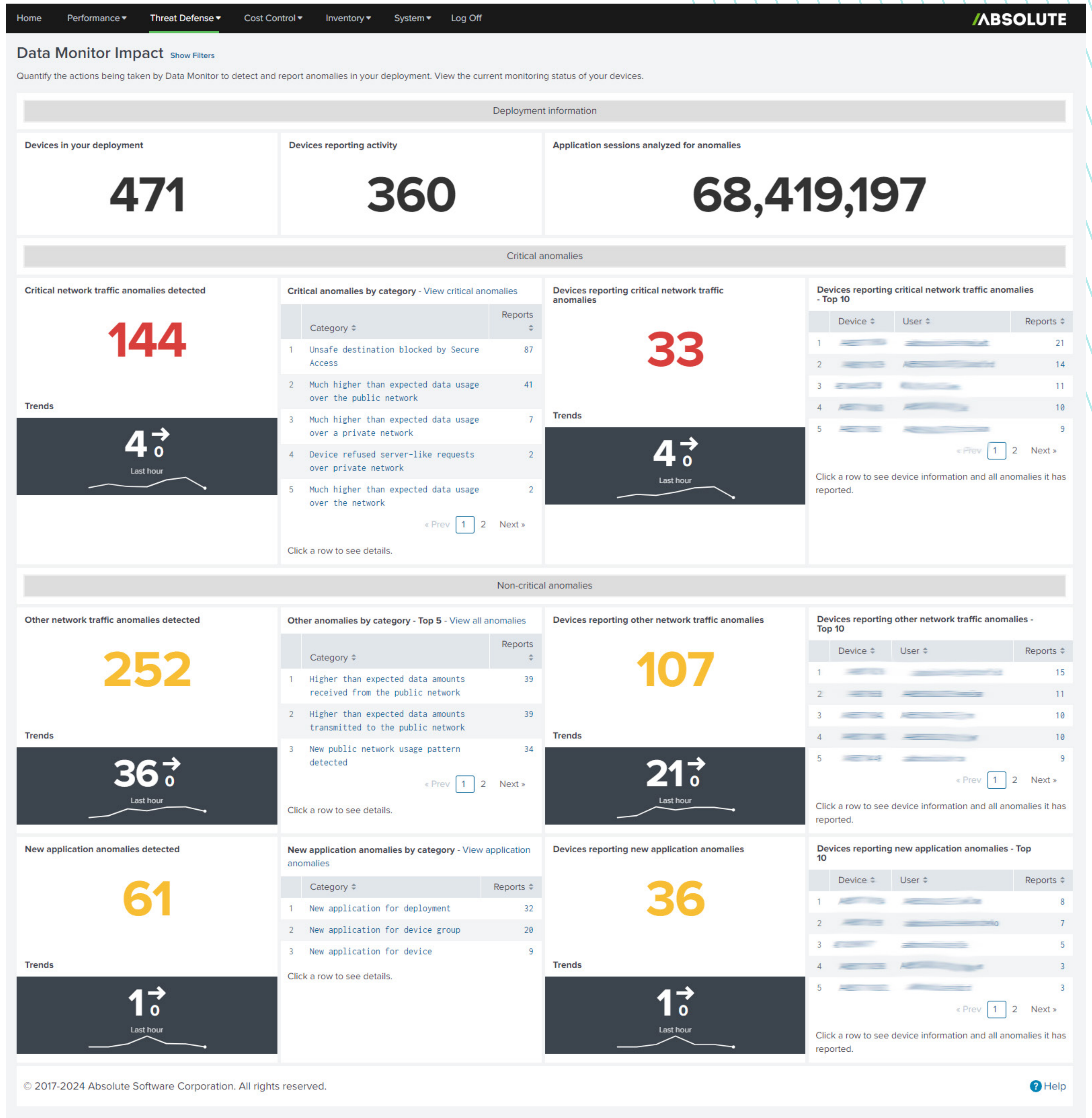
Benefits

Enhanced User Experience	Monitor endpoints, users, networks and applications with advanced AI – without routing traffic to the cloud for analysis.
Proactive Alerts	Quickly receive proactive alerts to suspicious zero-day behaviors without continuously monitoring dashboards.
Better Security Awareness	Gain deeper understanding of user, endpoint, network, and application activity for improved security posture.
Faster Threat Detection	Automatically identify and respond to threats before they can cause significant damage.
Reduced Investigation Time	Focus on the most critical threats with prioritized alerts based on risk.
Eliminate Alert Fatigue	Eliminate false positive fatigue caused by traditional security tools with AI Threat Insights' focus on real vulnerabilities, threats, or suspicious activities.
Quick Threat Context	Facilitate rapid investigations with integrated dashboards in Insights for Network, ad hoc search capabilities, and drill-down activities to individual devices and processes.

Continuous Monitoring

AI Threat Insights continuously monitors your organization's user, endpoint, network, and application behavior. Using advanced generative AI, signature analysis, heuristics and machine learning, it monitors each user's unique behavior, providing early detection of suspicious activities.

AI Threat Insights generates configurable alerts in Secure Access with rich context and direct links to detailed Insights for Network dashboards, empowering security teams to prioritize and investigate potential threats. As new threats emerge and user behavior evolves, AI Threat Insights automatically modifies its baseline for each user's device and potential threat profiles, ensuring that each organization's defenses remain continuously updated.



Data Monitor Impact Show Filters

Quantify the actions being taken by Data Monitor to detect and report anomalies in your deployment. View the current monitoring status of your devices.

Deployment information

Devices in your deployment: 471

Devices reporting activity: 360

Application sessions analyzed for anomalies: 68,419,197

Critical anomalies

Critical network traffic anomalies detected: 144

Trends: 4 → 0 Last hour

Critical anomalies by category - View critical anomalies

	Category ⇕	Reports ⇕
1	Unsafe destination blocked by Secure Access	87
2	Much higher than expected data usage over the public network	41
3	Much higher than expected data usage over a private network	7
4	Device refused server-like requests over private network	2
5	Much higher than expected data usage over the network	2

« Prev 1 2 Next »

Click a row to see details.

Devices reporting critical network traffic anomalies: 33

Trends: 4 → 0 Last hour

Devices reporting critical network traffic anomalies - Top 10

	Device ⇕	User ⇕	Reports ⇕
1	[redacted]	[redacted]	21
2	[redacted]	[redacted]	14
3	[redacted]	[redacted]	11
4	[redacted]	[redacted]	10
5	[redacted]	[redacted]	9

« Prev 1 2 Next »

Click a row to see device information and all anomalies it has reported.

Non-critical anomalies

Other network traffic anomalies detected: 252

Trends: 36 → 0 Last hour

Other anomalies by category - Top 5 - View all anomalies

	Category ⇕	Reports ⇕
1	Higher than expected data amounts received from the public network	39
2	Higher than expected data amounts transmitted to the public network	39
3	New public network usage pattern detected	34

« Prev 1 2 Next »

Click a row to see details.

Devices reporting other network traffic anomalies: 107

Trends: 21 → 0 Last hour

Devices reporting other network traffic anomalies - Top 10

	Device ⇕	User ⇕	Reports ⇕
1	[redacted]	[redacted]	15
2	[redacted]	[redacted]	11
3	[redacted]	[redacted]	10
4	[redacted]	[redacted]	10
5	[redacted]	[redacted]	9

« Prev 1 2 Next »

Click a row to see device information and all anomalies it has reported.

New application anomalies detected: 61

Trends: 1 → 0 Last hour

New application anomalies by category - View application anomalies

	Category ⇕	Reports ⇕
1	New application for deployment	32
2	New application for device group	20
3	New application for device	9

Click a row to see details.

Devices reporting new application anomalies: 36

Trends: 1 → 0 Last hour

Devices reporting new application anomalies - Top 10

	Device ⇕	User ⇕	Reports ⇕
1	[redacted]	[redacted]	8
2	[redacted]	[redacted]	7
3	[redacted]	[redacted]	5
4	[redacted]	[redacted]	3
5	[redacted]	[redacted]	3

« Prev 1 2 Next »

Click a row to see device information and all anomalies it has reported.

© 2017-2024 Absolute Software Corporation. All rights reserved.

? Help

Insights for Network dashboards showing impact, critical, and non-critical vulnerabilities, threats, or suspicious activities

Data exfiltration	Device usage at unusual times
New applications generating network traffic	Higher amounts of data than expected
Unsafe application and web browsing behavior	Higher than expected network activity
Malicious network port scanning	New or anomalous network usage patterns
Possible denial of service attacks	Device acting as a server
Suspicious network usage	Device refusing server-like requests

Examples of security vulnerabilities, threats, and suspicious activities detected

Suspicious Activity Identified

AI Threat Insights continuously monitors and tracks activity, providing early detection of suspicious activities that might slip past traditional signature-based tools. Using advanced AI and deep flow analysis, a virtually unlimited number of suspicious activities can be identified.

Advanced Threat Detection and User and Entity Behavior Analytics (UEBA)

Zero-day threats can be especially harmful and can cause outages, data loss, and even promote ransomware. AI Threat Insights helps IT by delivering proactive risk-based alerts on configurable parameters that deliver actionable information quickly.

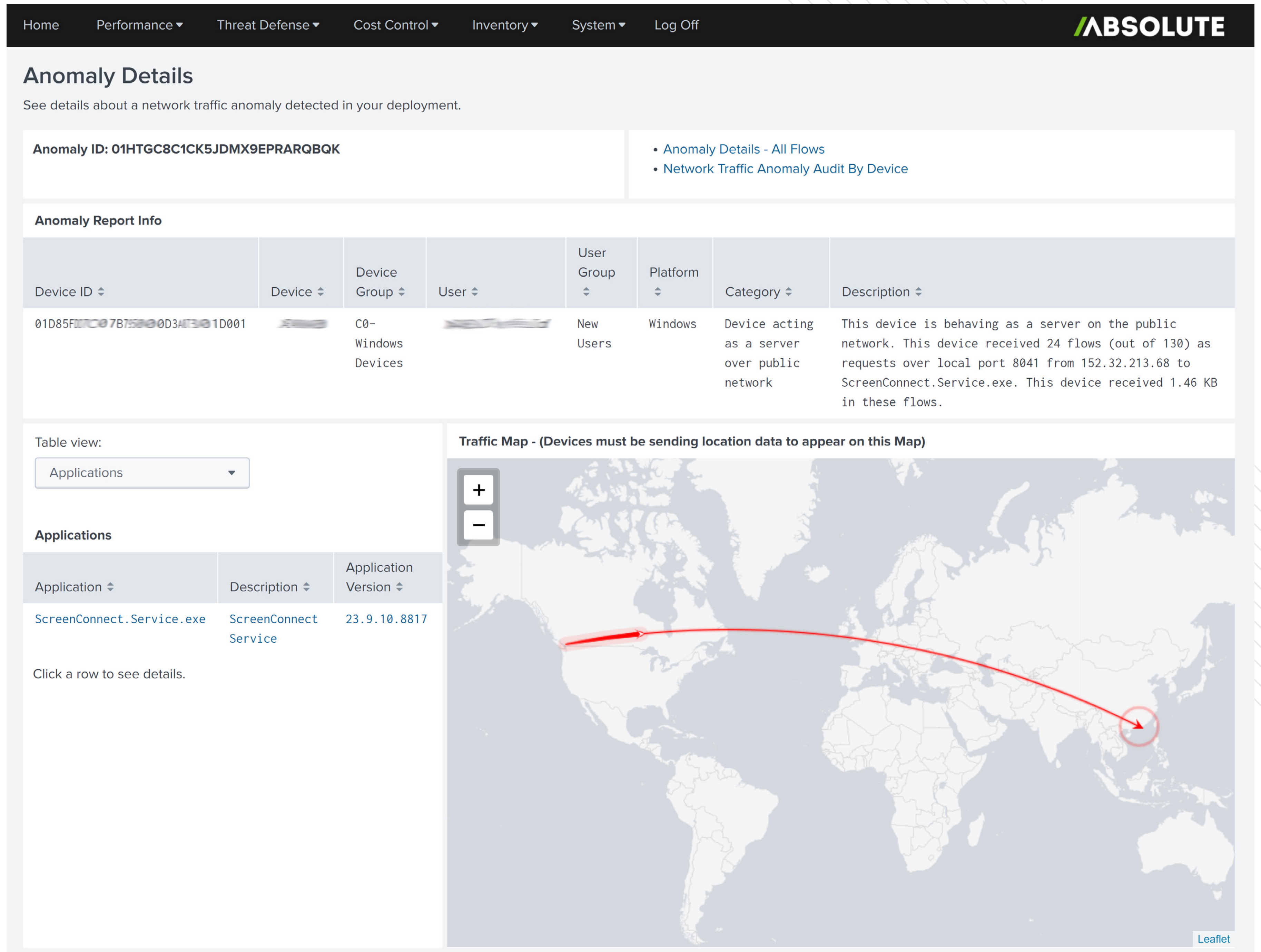
- Spot vulnerabilities, threats, and suspicious activities at-a-glance, pinpointing individual users, devices, networks, and applications that may indicate a problem
- Flag or alert on suspicious internet browsing and network activity
- Block or deny suspicious activity by policy action
- Drill down to user, device, and flow data for fast problem identification and resolution
- Notify and track movement of large amounts of data from internal to external systems
- Detect possible data exfiltration activities and identify geographic locations directly on maps
- Combat phishing, smishing, distributed denial of service (DDoS), malware, and advanced persistent threats (APTs) with AI-powered analytics
- Protect against data loss and leakage and mitigate risk at scale with data-driven insights
- Enable better situational awareness and rapid responses to suspicious behaviors and issues before they become problems
- Speed problem identification, resolution, and troubleshooting
- Identify suspicious traffic to/from web servers, file servers, and other network endpoints
- Determine possible lateral movement, such as multiple users or devices with similar unexpected activity
- Flag user, device, or application access to destinations with high risk and poor reputations
- Streamline multi-step investigations by helping trace suspicious activity from the application to the individual device

Proactive Security for Organizations of All Sizes

AI Threat Insights represents a significant advance against increasingly complex and numerous security threats. It is a proactive alerting system that is tightly integrated with Absolute's Secure Access SSE platform and is designed to aid IT departments in preventing security issues from becoming problems.

Unlike other solutions, Secure Access Security Service Edge agents do not require hair pinning traffic through the cloud. This improves user experience and application performance by lowering latency, reducing network hops, and avoiding costly traffic choke points. Administrators and users gain control and visibility both inside and outside Absolute's secure, optimized tunnel and ensures that each organization's data is uniquely analyzed, detecting only threats that apply directly to your organization.

By incorporating comprehensive AI and ML technologies, Absolute's AI Threat Insights gives businesses the upper hand against a complex and high-risk security landscape, reducing the attack surface and keeping workers safe and productive.



Anomaly Details

See details about a network traffic anomaly detected in your deployment.

Anomaly ID: 01HTGC8C1CK5JDMX9EPRARQBQK

- Anomaly Details - All Flows
- Network Traffic Anomaly Audit By Device

Anomaly Report Info

Device ID ⇕	Device ⇕	Device Group ⇕	User ⇕	User Group ⇕	Platform ⇕	Category ⇕	Description ⇕
01D85F[redacted]1D001	[redacted]	C0-Windows Devices	[redacted]	New Users	Windows	Device acting as a server over public network	This device is behaving as a server on the public network. This device received 24 flows (out of 130) as requests over local port 8041 from 152.32.213.68 to ScreenConnect.Service.exe. This device received 1.46 KB in these flows.

Table view:

Applications ▾

Applications

Application ⇕	Description ⇕	Application Version ⇕
ScreenConnect.Service.exe	ScreenConnect Service	23.9.10.8817

Click a row to see details.

Traffic Map - (Devices must be sending location data to appear on this Map)

Threat details with actionable information

Absolute Security is partnered with more than 28 of the world's leading endpoint device manufacturers, embedded in the firmware of 600 million devices, trusted by 21,000 global enterprises, and licensed across 14 million PC users. With the Absolute Security Cyber Resilience Platform integrated into their digital enterprise, customers ensure their mobile and hybrid workforces connect securely and seamlessly from anywhere in the world and that business operations recover quickly following cyber disruptions and attacks. Our award-winning capabilities have earned recognition and leadership status across multiple technology categories, including **Zero Trust Network Access (ZTNA)**, **Endpoint Security**, **Security Services Edge (SSE)**, Firmware-Embedded Persistence, **Automated Security Control Assessment (ASCA)**, and **Zero Trust Platforms**.

Request a Demo